Randomized Half-Ideal Cipher on Groups with applications to UC (a)PAKE

Bruno Freitas Dos Santos[0009−0009−5474−0008], Yanqi Gu[0000−0001−6577−2704], and Stanislaw Jarecki[0000−0002−5055−2407]

University of California, Irvine. Email: {brunof,yanqig1,sjarecki}@uci.edu

Abstract. An Ideal Cipher (IC) is a cipher where each key defines a random permutation on the domain. Ideal Cipher on a group has many attractive applications, e.g., the *Encrypted Key Exchange* (EKE) protocol for Password Authenticated Key Exchange (PAKE) [10], or asymmetric PAKE (aPAKE) [41, 37]. However, known constructions for IC on a group domain all have drawbacks, including key leakage from timing information [15], requiring 4 hash-onto-group operations if IC is an 8-round Feistel [27], and limiting the domain to half the group [12] or using variable-time encoding [57, 49] if IC is implemented via (quasi-) bijections from groups to bitstrings [41].

We propose an IC relaxation called a *(Randomized) Half-Ideal Cipher* (HIC), and we show that HIC on a group can be realized by a *modified 2-round Feistel* (m2F), at a cost of 1 hash-onto-group operation, which beats existing IC constructions in versatility and computational cost. HIC weakens IC properties by letting part of the ciphertext be non-random, but we exemplify that it can be used as a drop-in replacement for IC by showing that EKE [10] and aPAKE of [41] realize respectively UC PAKE and UC aPAKE even if they use HIC instead of IC. The m2F construction can also serve as IC domain extension, because m2F constructs HIC on domain D from an RO-indifferentiable hash onto D and an IC on 2κ-bit strings, for κ a security parameter. One application of such extender is a modular lattice-based UC PAKE using EKE instantiated with HIC and anonymous lattice-based KEM.

1 Introduction

The Ideal Cipher Model (ICM) dates back to the work of Shannon [56], and it models a block cipher as an Ideal Cipher (IC) oracle, where every key, even chosen by the attacker, defines an independent random permutation.[1] Formally, an efficient adversary who evaluates a block cipher on any key k of its choice cannot distinguish computing the cipher on that key in the forward and backward direction from an interaction with oracles $E_k(\cdot)$ and $E_k^{-1}(\cdot)$, where $\{E_i\}$ is a family of random permutations on the cipher domain. The Ideal Cipher Model has seen a variety of applications in cryptographic analysis, e.g. [58, 54, 34, 55,

[1] This is an extended version of a paper which appears in Eurocrypt'23 [36].